PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L

A2

(11) Numéro de publication internationale: WO 00/46947

(43) Date de publication internationale: 10 août 2000 (10.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00189

(22) Date de dépôt international: 27 janvier 2000 (27.01.00)

(30) Données relatives à la priorité:

| | | |
|---|---|---|
| 99/01065 | 27 janvier 1999 (27.01.99) | FR |
| 99/03770 | 23 mars 1999 (23.03.99) | FR |
| 99/12465 | 1er octobre 1999 (01.10.99) | FR |
| 99/12467 | 1er octobre 1999 (01.10.99) | FR |
| 99/12468 | 1er octobre 1999 (01.10.99) | FR |


(71) Déposants (*pour tous les Etats désignés sauf US*): FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F–75015 Paris (FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour–sur–Glane, F–75732 Paris Cedex 15 (FR). MATH RIZK [BE/BE]; Verte Voie, 20 Boîte 5, B–1348 Louvain–la–Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants (*US seulement*): GUILLOU, Louis [FR/FR]; 16, rue de l'Ise, F–35230 Bourgbarre (FR). QUISQUATER, Jean–Jacques [BE/BE]; 3, avenue des Canards, B–1640 Rhode Saint Genese (BE).

(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F–35700 Rennes (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

*Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.*

(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY AND/OR THE AUTHENTICITY OF A MESSAGE USING SPECIFIC PRIME FACTORS

(54) Titre: PROCEDE, SYSTEME, DISPOSITIF DESTINES A PROUVER L'AUTHENTICITE D'UNE ENTITE ET/OU L'INTEGRITE ET/OU L'AUTHENTICITE D'UN MESSAGE AUX MOYENS DE FACTEURS PREMIERS PARTICULIERS

(57) Abstract

The proof is provided by means of the following parameters: a public module n formed by the product of f prime factors $p_i$, f>2; a public superscript v; m base numbers $g_i$, m>1. The base numbers $g_i$ are such that the two equations: $x^2 \equiv g_i \bmod n$ and $x^2 \equiv -g_i \bmod n$ cannot be solved in x in the ring of integers modulo n, and such that the equation $x^v \equiv g_i^2 \bmod n$ can be solved in x in the ring of integers modulo n in the case where the public superscript v is in the form $v = 2^k$, wherein k is a security parameter.

(57) Abrégé

La preuve est établie au moyen des paramètres suivants: un module public n constitué par le produit de f facteurs premiers, $p_i$,f>2, un exposant public v, m nombres de base, $g_i$, m>1. Les nombres de base $g_i$, sont tels que les deux équations: $x^2 \equiv g_i \bmod n$ et $x^2 \equiv g_i \bmod n$ n'ont pas de solution en x dans l'anneau des entiers modulo n, et tel que l'équation $x^v \equiv -g_i^2 \bmod n$ a des solutions en x dans l'anneau des entiers modulo n dans le cas, où l'exposant public v est de la forme $v = 2^k$ où k est un paramètre de sécurité.